



Office for
Nuclear Regulation

Developing a national strategy to address the cyber insider risk in the nuclear sector

Romin Partovnia, Cyber Security & Information Assurance Inspector, ONR

National Strategy; Key Stakeholders

Nuclear
Operators


ONR

Government

International
Engagement

Technical
Authorities

Government; Legislation



Energy Act 2013

CHAPTER 32

CONTENTS

PART 1

DECARBONISATION

- 1 Decarbonisation target range
- 2 Matters to be taken into account
- 3 Further duties of the Secretary of State
- 4 Meaning and calculation of "carbon intensity of electricity generation in the United Kingdom"

PART 2

ELECTRICITY MARKET REFORM

CHAPTER 1

GENERAL CONSIDERATIONS

- 5 General considerations relating to this Part

CHAPTER 2

CONTRACTS FOR DIFFERENCE

- 6 Regulations to encourage low carbon electricity generation
- 7 Designation of a CFD counterparty
- 8 Duties of a CFD counterparty
- 9 Supplier obligation
- 10 Direction to offer to contract
- 11 Standard terms
- 12 CFD authorisation
- 13 Allocation of CFDs
- 14 CFD authorisation: offer to contract on standard terms

SI 2003/403 Page 1

2003 No. 403

ATOMIC ENERGY AND RADIOACTIVE SUBSTANCES

The Nuclear Industries Security Regulations 2003

Thomson Reuters (Legal) Limited.

UK Statutory Instruments Crown Copyright. Reproduced by permission of Her Majesty's Stationery Office.

<i>Made</i>	<i>26th February 2003</i>
<i>Laid before Parliament</i>	<i>28th February 2003</i>
<i>Coming into force</i>	
<i>Part 3 and Parts 1 and 5 so far as they apply for the purposes of Part 3</i>	<i>22nd September 2003</i>
<i>Remainder</i>	<i>22nd March 2003</i>

The Secretary of State, in exercise of the powers conferred by sections 15(1), (2), (3)(c), (4)(a), (5)(a) and (b), 50(1) and 82(3)(a) of, and paragraphs 1(1)(a) and (b) and (2), 3(1) and (2), 4(1), 15(1), 16 and 21(a) of Schedule 3 to, the Health and Safety at Work etc. Act 1974¹ and sections 76(7) and 77(1) to (4) of the Anti-terrorism, Crime and Security Act 2001, and after consulting the Health and Safety Commission, such other bodies as appear to her to be appropriate (in accordance with section 50(1) of that Act of 1974) and such other persons as she considers appropriate (in accordance with section 77(5) of that Act of 2001), hereby makes the following Regulations:—

Notes

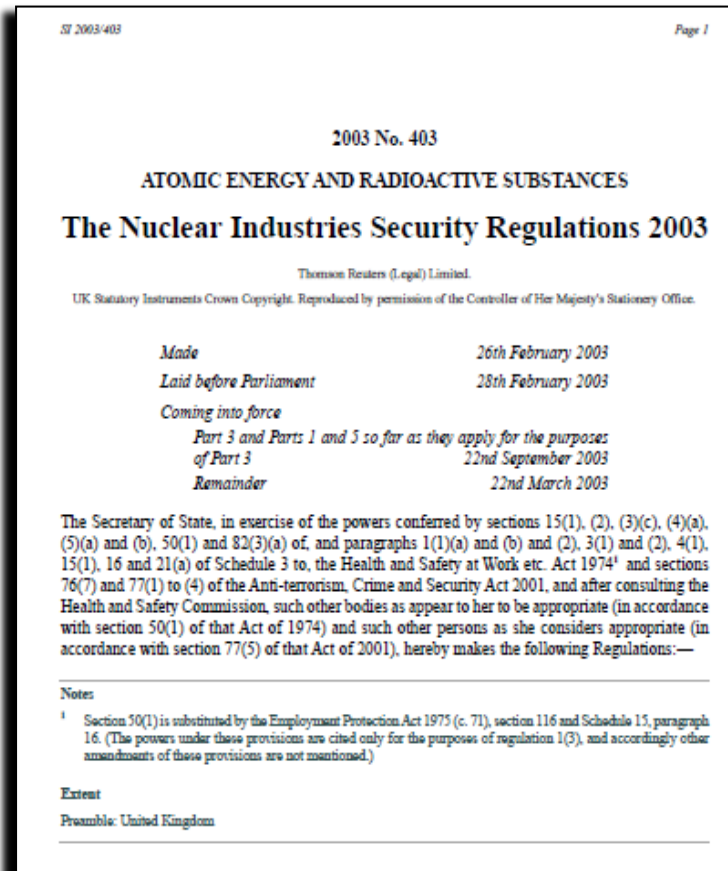
¹ Section 50(1) is substituted by the Employment Protection Act 1975 (c. 71), section 116 and Schedule 15, paragraph 16. (The powers under these provisions are cited only for the purposes of regulation 1(3), and accordingly other amendments of these provisions are not mentioned.)

Extent

Preamble: United Kingdom

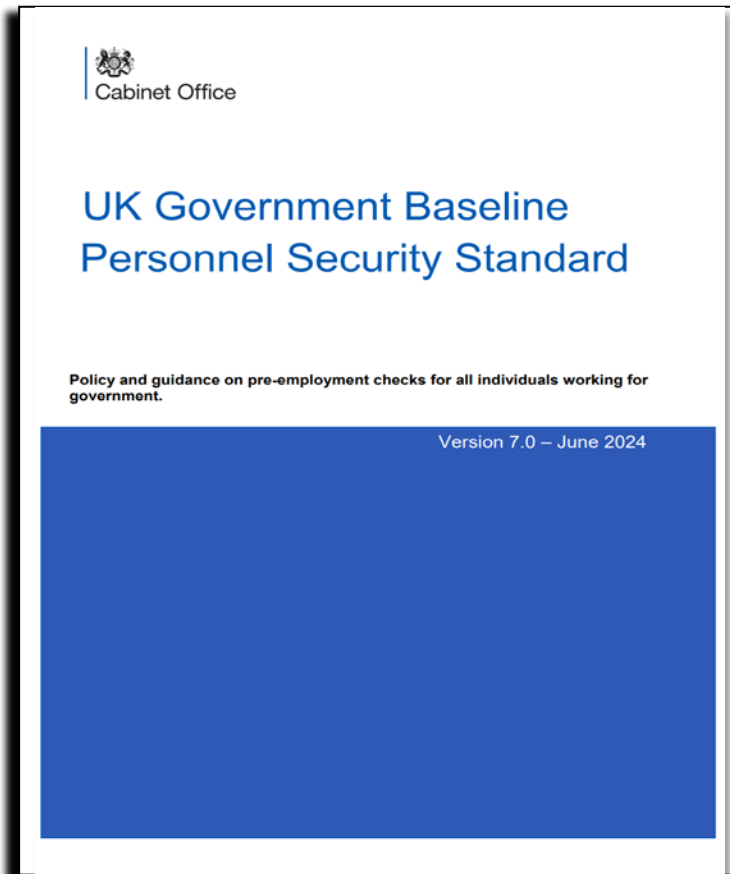
Government; Approved Security Plan.

Regulation 4 “Standards, Procedures and Arrangement....”

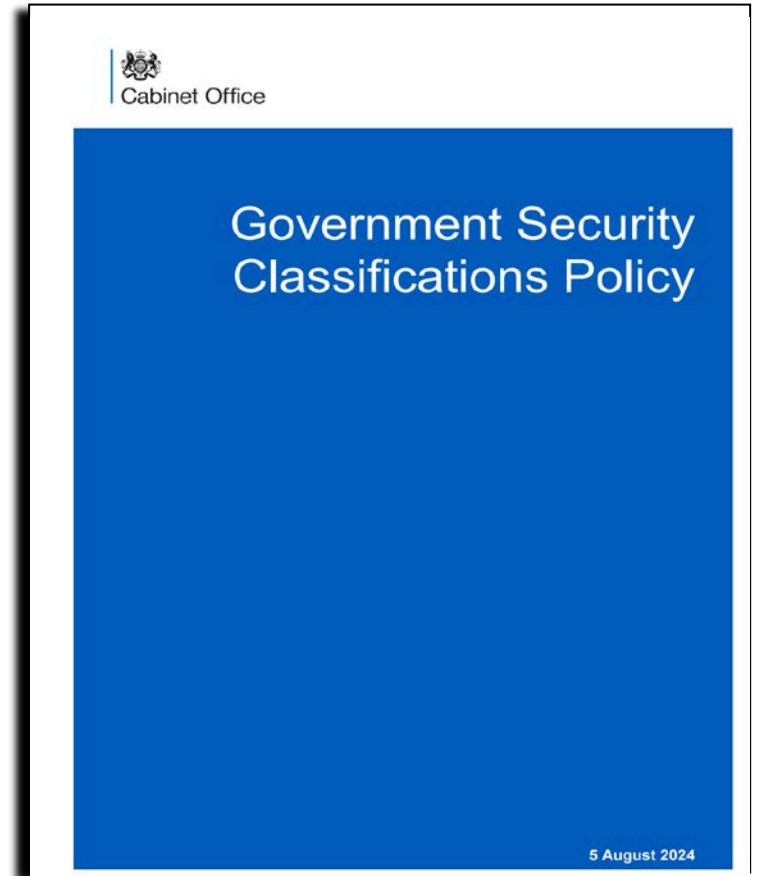


Government; National Policy

Regulation 9 – Requirement for Approval of Relevant Personnel



United Kingdom Security Vetting



Government; Design Basis Threat (DBT)

Regulation 22: maintain such security standards, procedures and arrangements as are necessary for the purpose of minimising the risk....

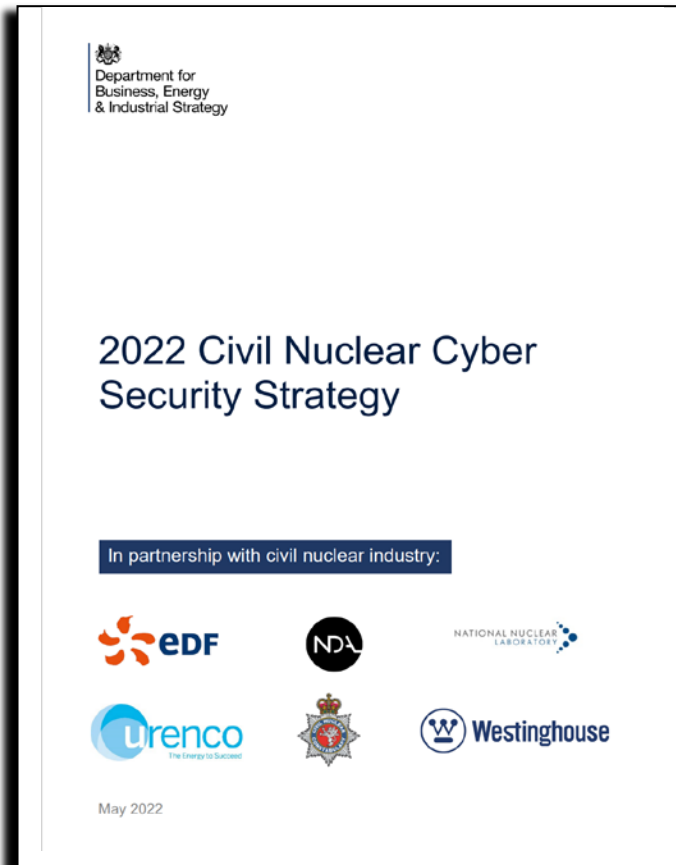


Civil Nuclear Sector
Design Basis Threat (DBT)

Classification: SECRET

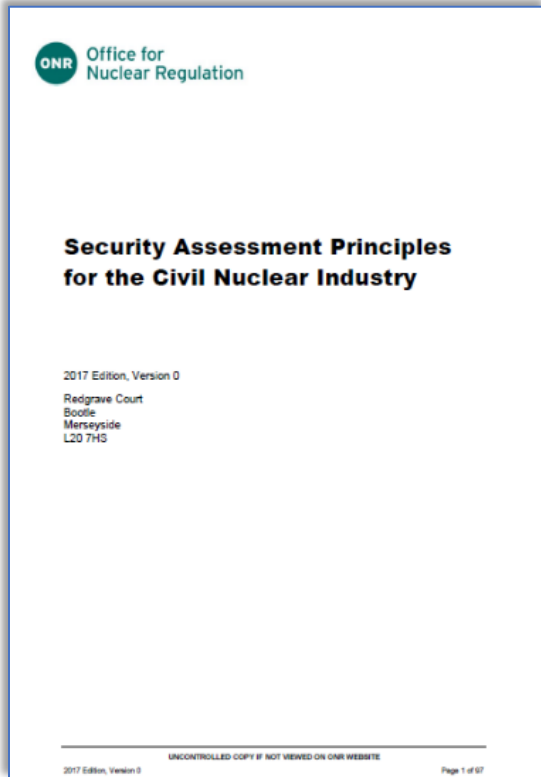
A DBT describes the capabilities of potential insider and external adversaries who might attempt unauthorized removal of nuclear and other radioactive material or sabotage. The operator's physical protection system is designed and evaluated on the basis of the DBT.

Government; Civil Nuclear Sector Cyber Strategy



- Cyber security should be prioritised amongst wider organisational safety, environmental and financial risks, as part of a holistic risk management approach
- Cybersecurity is a product of culture rather than a set of isolated controls. Success relies on embedding and sustaining strong cyber security awareness
- the importance of strategic enablers such as leadership, governance and competence must be recognised. ONR to ensure appropriate engagement and accountability of cyber security at a senior level
- Ensure cyber security is embedded into the deployment of new nuclear technologies

Regulation; Security Assessment Principles (SyAPs)



- The SyAPs provide the essential foundation for the introduction of outcome focussed regulation for all constituent security disciplines: physical, personnel, transport, and cyber security and information assurance
1. Leadership and Management
 2. Organisational Culture
 3. Management of Human Performance
 4. Nuclear Supply Chain
 5. Reliability, Resilience and Sustainability
 6. Physical protection system
 7. Cyber Security
 8. Workforce Trustworthiness
 9. Policing and guarding
 10. Emergency response

Regulation; Fundamental Security Principles

Fundamental Security Principle 7; Cyber Security and Information Assurance

- Dutyholders must implement and maintain effective cyber security and information assurance arrangements that integrate technical and procedural controls to protect the confidentiality, integrity and availability of SNI and technology.

Security Delivery Principles

- Dutyholders should maintain arrangements to ensure that CS&IA risk is managed effectively
- Dutyholders should maintain the confidentiality, integrity and availability of sensitive nuclear information and associated assets.
- Dutyholders should ensure their operational and information technology is secure and resilient to cyber threats by integrating security into design, implementation, operation and maintenance activities

Technical Assessment Guide (TAG) Information Security

- The CS&IA Strategy should be underpinned by a comprehensive policy structure. The topics within the policy should include, but it not limited to, Personnel Security and management, social engineering, security training, acceptable use
- Dutyholders should undertake inspections and audits of third party suppliers , including workforce trustworthiness
- Comprehensive site physical security assessment will already have been completed to assess the risk of malicious acts to Nuclear Material (NM), Other Radioactive Material (ORM) and nuclear facilities. The risk assessment should also reflect the insider threat and consider the unique problem this poses due to the advantages they have over an adversary
- Dutyholders should consider controls that will deter, delay, detect, assess and respond to physical risks, including those posed by insider

Regulation; Fundamental Security Principles

Fundamental Security Principle 8; Workforce Trustworthiness

- Dutyholders must implement and maintain a regime of workforce trustworthiness to reduce the risks posed by insider activity

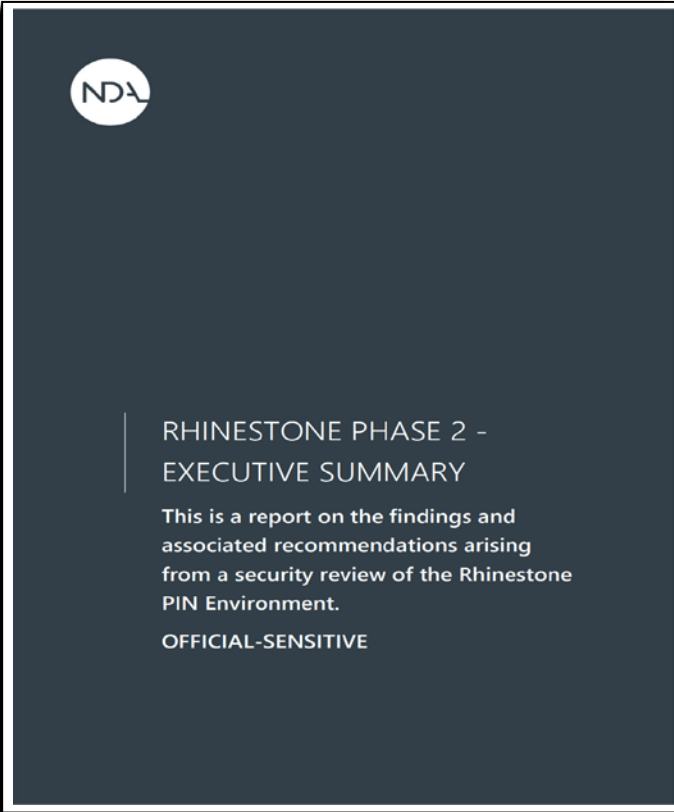
Security Delivery Principle

- Dutyholders should ensure that human resources, occupational health and security departments cooperate to facilitate effective screening, vetting and ongoing personnel security arrangements for the workforce
- Dutyholders should deliver the appropriate combination of recruitment checks and vetting to satisfy themselves of the honesty and integrity of their potential workforce.

Technical Assessment Guide (TAG) Information Security

- Delivering vetting and ongoing personnel security arrangements
- Pre-employment screening and national security vetting
- Ongoing personnel security aftercare

Regulation; Security Testing Direction



Internal Purple team (Insider detection)

28 January – 08 February 2024

120 Tactics, Techniques and Procedures;

1. Create users account
2. Add account to privileged membership group
3. Disable anti-virus
4. Create Windows Service

Technical Authorities; Guidance



The screenshot shows the top navigation bar of the National Cyber Security Centre website. The logo is on the left, and navigation links include 'Home', 'Information for...', 'Advice & guidance', 'Education & skills', and 'Products & services'. A secondary menu contains 'ABOUT NCSC' and 'CISP'. Below the navigation, a 'GUIDANCE' tag is visible. The main heading is 'Reducing data exfiltration by malicious insiders', followed by a sub-heading: 'Advice and recommendations for mitigating this type of insider behaviour.' The bottom of the page features a graphic with green and blue geometric shapes and circuit-like patterns.

National Cyber Security Centre

ABOUT NCSC CISP

Home Information for... Advice & guidance Education & skills Products & services

GUIDANCE

Reducing data exfiltration by malicious insiders

Advice and recommendations for mitigating this type of insider behaviour.



The screenshot shows the top navigation bar of the National Cyber Security Centre website. The logo is on the left, and navigation links include 'Home', 'Information for...', 'Advice & guidance', 'Education & skills', 'Products & services', and 'New'. A secondary menu contains 'ABOUT NCSC', 'CISP', and 'REPO'. Below the navigation, an 'INFORMATION' tag is visible. The main heading is 'Exercise in a Box', followed by a sub-heading: 'An online tool which helps organisations find out how resilient they are to cyber attacks and practise their response in a safe environment'. Below the text is an illustration of an open cardboard box with a padlock icon on the left and a checklist icon on the right.

National Cyber Security Centre

ABOUT NCSC CISP REPO

Home Information for... Advice & guidance Education & skills Products & services New

INFORMATION

Exercise in a Box

An online tool which helps organisations find out how resilient they are to cyber attacks and practise their response in a safe environment



Technical Authorities; National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF)

OBJECTIVE	PRINCIPLE
A: Managing Security Risk	A1 Governance
	A2 Risk Management
	A3 Asset Management
	A4 Supply Chain
B: Protecting Against Cyber Attack	B1 Service Protection Policies and Processes
	B2 Identity and Access Control
	B3 Data Security
	B4 System Security
	B5 Resilient Networks and Systems
	B6 Staff Awareness and Training
C: Detecting Cyber Security Events	C1 Security Monitoring
	C2 Proactive Security Event Discovery
D: Minimising the Impact of Cyber Security Incidents	D1 Response and Recovery Planning
	D2 Lessons Learned

B2: Identify: Only authorised and individually authenticated users can physically access and logically connect to your network.

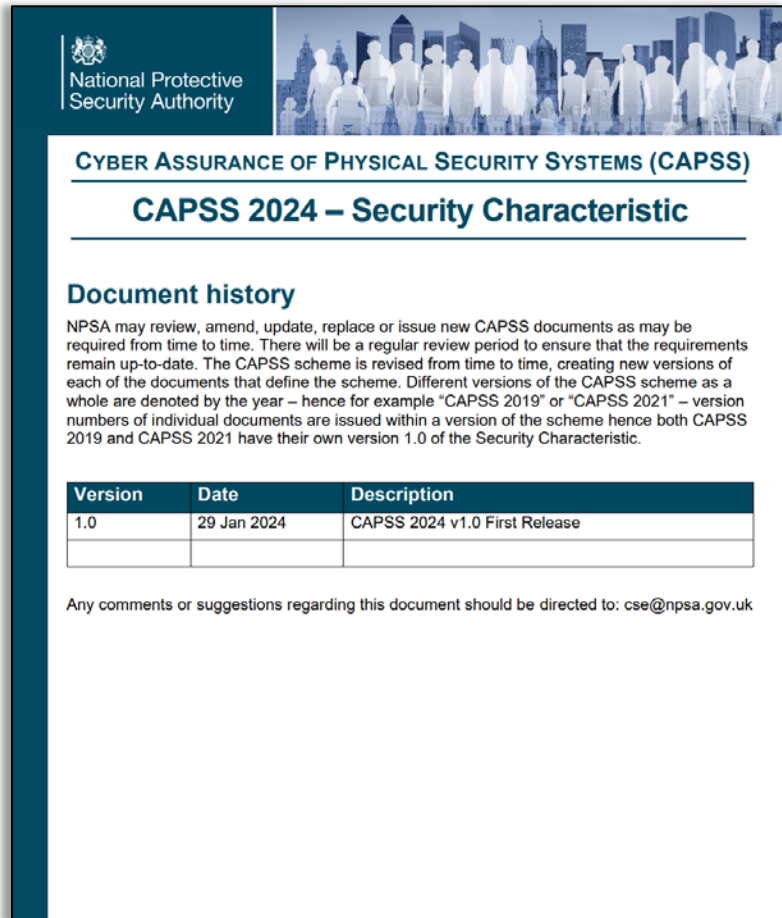
B2: Privileged User Management: Privileged user access is closely monitored and managed.

D3:Secure by Design: Network and information systems are segregated into appropriate security zones

C1:Secure Monitoring: Log collection capture staff use of corporate systems

Technical Authorities; National Protective Security Authority (NPSA)

NPSA's collection of ongoing personnel security guidance and tools can be used to help an organisation develop and plan effective practices for countering the insider threat and maintaining a motivated, engaged and productive workforce



The screenshot shows the NPSA logo and the title 'CYBER ASSURANCE OF PHYSICAL SECURITY SYSTEMS (CAPSS) CAPSS 2024 – Security Characteristic'. It includes a 'Document history' section with a paragraph explaining the review process and a table with one entry: Version 1.0, Date 29 Jan 2024, Description CAPSS 2024 v1.0 First Release. A footer note directs comments to cse@npsa.gov.uk.

National Protective Security Authority

CYBER ASSURANCE OF PHYSICAL SECURITY SYSTEMS (CAPSS)

CAPSS 2024 – Security Characteristic

Document history

NPSA may review, amend, update, replace or issue new CAPSS documents as may be required from time to time. There will be a regular review period to ensure that the requirements remain up-to-date. The CAPSS scheme is revised from time to time, creating new versions of each of the documents that define the scheme. Different versions of the CAPSS scheme as a whole are denoted by the year – hence for example "CAPSS 2019" or "CAPSS 2021" – version numbers of individual documents are issued within a version of the scheme hence both CAPSS 2019 and CAPSS 2021 have their own version 1.0 of the Security Characteristic.

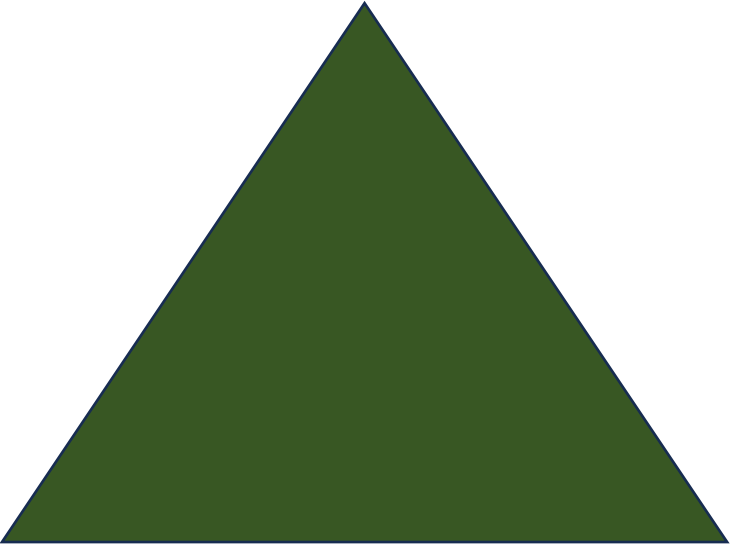
Version	Date	Description
1.0	29 Jan 2024	CAPSS 2024 v1.0 First Release

Any comments or suggestions regarding this document should be directed to: cse@npsa.gov.uk

- Encrypt communication traffic over untrusted links
- Encrypt sensitive data
- Log all relevant events
- MFA for privileged accounts
- Implement tamper response
- Ensure product security configuration can be backed up

Nuclear Operators

- Chief Information Security Officers (CISO) Working Groups



- Insider Risk Working Groups

- Supply Chain Security Assurance Working Group

International; Western European Nuclear Regulators Association (WENRA) European Nuclear Security Regulators Association (ENSRA)

ENSRA-WENRA Working Group on Cyber Security.

- Analysing and summarising the current state of cyber security
- Exchanging current best practice
- Developing reference levels to harmonize a coordinated approach to cyber security.
- Developing a common security sharing platform.

National Strategy; Conclusion

Government

- TEA2013 and NISR
- DBT
- Cyber Strategy
- National Policy (i.e. Vetting)

ONR

- Security Assessment Principles
- Technical Assessment Guides
- Security Testing

Technical
authorities

- Guidance and Incident Response Exercise
- Cyber Assessment Framework
- CAPPS Standard

Operators

- Cross industry working groups

International

ENSRA-WENRA Working
Group on Cyber Security

Romin.Partovnia@onr.gov.uk

NISR Legislation: <https://www.legislation.gov.uk/uksi/2003/403/contents/made>

National Security Clearance Policy: <https://www.gov.uk/government/publications/united-kingdom-security-vetting-clearance-levels/national-security-vetting-clearance-levels>

National Classification Policy: <https://www.gov.uk/government/publications/government-security-classifications/government-security-classifications-policy-html>

Civil nuclear sector cyber security strategy 2022: <https://www.gov.uk/government/publications/civil-nuclear-cyber-security-strategy-2022>

ONR Security Assessment Principles: <https://www.onr.org.uk/publications/regulatory-guidance/regulatory-assessment-and-permissioning/security-assessment-principles-syaps/security-assessment-principles-syaps/>

ONR Technical Assessment Guidelines: <https://www.onr.org.uk/publications/regulatory-guidance/regulatory-assessment-and-permissioning/technical-assessment-guides-tags/nuclear-security-tags/technical-assessment-guides-tags-nuclear-security/>

NCSC Reducing data exfiltration by malicious insider: <https://www.ncsc.gov.uk/guidance/reducing-data-exfiltration-by-malicious-insiders>

NCSC Exercise in a Box: <https://www.ncsc.gov.uk/information/exercise-in-a-box>

NCSC Cyber Assessment Framework: <https://www.ncsc.gov.uk/collection/cyber-assessment-framework>

NSPA CAPPS Standard: <https://www.npsa.gov.uk/cyber-assurance-physical-security-systems-capss>